REMARKS/ARGUMENTS

The applicant acknowledges, with thanks, receipt of the Office Action that was mailed on October 4, 2007. This amendment is responsive to the October 4, 2007, Office Action. Claims 1, 3, 4, 11, 12, 17 and 24 have been amended. The subject matter of determining whether a shared secret between a first party and a second party exists is not new matter, as it is disclosed in paragraphs 118 and 119 of the original specification (*cf.* reference char 610 of Fig. 6).

SUBSTANCE OF INTERVIEW

The applicant acknowledges, with thanks, the interview conducted on 03 August 2007. Attending the interview was the examiner and the undersigned. The interview was conducted by telephone. No exhibits or demonstrations were conducted. Discussed were claims 1 and 24, and prior art references Funk and Schneier. The general thrust of the discussion was the purpose, content and distribution of the protected access credential (PAC) and to distinguish from Funk and Schneier. No other pertinent matters were discussed. No agreement was reached.

NON-ART MATTERS

Claims 24 and 26 were objected to for the following informality. Claims 24 and 26 do not have a consistent use of "wireless device" versus "wireless client." The first recitation of wireless client refers to "the wireless client," which does not have antecedent basis. Accordingly, claim 24 has been amended to correct the informality and withdrawal of the objection is requested.

Claims 1-12, 14-21, 24, 26 and 27 were rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claims contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor, at the time the application was filed, had possession of the claimed invention. Accordingly, claims 1, 17 and 24 have been amended to address the rejection and withdrawal of the rejection is requested.

PRIOR ART MATTERS

Claims 1-6, 9, 10, 12, 14-21, 24, 26, and 27 stand rejected under 35 U.S.C. 102(b) as being anticipated by Funk (Paul Funk, Simon Blake Wilson; "draft-ietf-pppext-eap-ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS);" Internet-Draft PPPEXT Working Group; 30 Nov. 2002, pp. 1-40). Claims 5-11 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Funk in view of Downnard (Downnard, Ian, "Public-key cryptography extensions into Kerberos," IEEE December 2002/January 2003, pp. 30-34). For reasons that will now be set forth , the claims as currently amended are neither anticipated by nor obvious in view of Funk and/or Downnard when considered alone or in combination.

Independent claims 1, 17, and 24, as now amended, recite determining whether a shared secret exists between a first party and a second party. Upon determining that a shared secret does not exist between the first and second parties, a first secure tunnel is established between the first party and the second party using asymmetric encryption. The shared secret is then provisioned through the first secure tunnel. If it determined that a shared secret already exists between a first party and a second party, a tunnel is established using symmetric encryption employing the shared secret. Once the shared secret is received (via a first tunnel established using asymmetric encryption), symmetric encryption using the shared secret is employed to establish one or more subsequent secure tunnels. Authentication is performed via the subsequent secure tunnels.

By contrast, Funk only uses asymmetric encryption to establish the secure tunnels for authentication. Funk discloses using a PKI architecture, which necessitates third party servers, and computational overhead for every authentication. Funk does not mention the possibility of distributing a shared secret within the tunnel and using the shared secret for establishing subsequent tunnel(s) via symmetric encryption.

The aforementioned deficiencies in Funk are not remedied by any teaching of Downard. The examiner relies on Downnard for using a protected access credential as a shared secret. However, Downnard does not mention obtaining the shared secret via a first secure tunnel established using asymmetric encryption and then using the shared secret to establish a subsequent secure tunnel between a first party and a second party using symmetric encryption. Thus, neither Funk nor Downnard, when taken alone or in combination, teach or suggest using

asymmetric encryption to establish a secure tunnel to acquire a shared secret, and then employing the shared secret to establish subsequent secure tunnels using symmetric encryption. Thus, neither Funk nor Downnard, alone or in combination, teach or suggest all of the elements of independent claims 1, 17 and 24.

Claims 2-12, 14-16 and 27 directly depend from claim 1 and therefore contain each and every element of claim 1. Claims 18-21 directly depend from claim 17 and therefore contain each and every element of claim 17. Claim 26 directly depends from claim 24 and therefore contains each and every element of claim 24. Therefore, claims 2-12, 14-16, 18-21 and 26-27 are neither anticipated nor obvious in view of Funk and/or Downnard for the reasons already set forth for claims 1, 17 and 24.

CONCLUSION

For the reasons just set forth, the applicant requests withdrawal of the objections and rejections. If there are any fees necessitated by the foregoing communication, the Commissioner is hereby authorized to charge such fees to our Deposit Account No. 50-0902, referencing our Docket No. 72255/00010.

Respectfully submitted,

Date: _____

Larry B. Donovan
Registration No. 47,230
TUCKER ELLIS & WEST LLP
1150 Huntington Bldg.
925 Euclid Ave.
Cleveland, Ohio 44115-1414
Customer No.: 23380
Tel.: (216) 696-3864
Fax: (216) 592-5009